SAGEM F@st^{TM} 1500WG

SAFRAN

SAGEM F@st^{TM} 1500WG

- Généralités F@st 1500WG
- Description physique
- Installation du modem routeur
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP

SAGEM F@st™ 1500WG - *Router ADSL WiFi multi utilisateurs*

Interface utilisateur

- **4 Eth 10/100BT**
- **802.11 b/g**
  - Securité : WEP, Filtrage Mac, WPA et futur 802.11i

Interface ADSL

- **ADSL**
  - Multimode : G.dmt Annex A, G.lite, ANSI T1.413
- **Interopérabilité**



SAGEM F@st™ 1500WG - *Wireless LAN*

Wireless Ethernet (802.11b/g)

- **11/54 Mps full-duplex - Bande de fréquence 2.4 GHz**
- **Sécurités :**
  - WEP avec clé de 64 ou 128 bits
  - WPA
  - MAC (Ethernet) vérification d'une Liste d'adresses
  - Arrêt du broadcast du SSID
  - Pas d'accès à la configuration par le port WiFi



SAGEM F@st^{TM} 1500WG - *Une offre complète*

SAGEM F@st^{TM} 1500 WG

- 4 Eth 10/100BT
- Wireless Eth 802.11b/g

Options pour les PC en connexion sans fil:

- Carte PCMCIA
- POD USB
- Dongle USB



SAGEM F@st™ 1500WG - *Caractéristiques (1)*

- **Bridge entre les interfaces LAN**
- **ATM : 8 VC**
  - UBR, CBR, VBRrt, VBRnrt
  - OAM management des cellules ATM
- **Encapsulation :**
  - PPPoA
  - PPPoE
  - RFC 1483 Routed / bridged
- **Mode simultané Routeur/bridge**
  - PPPoE pass-through



SAGEM F@st™ 1500WG - *Caractéristiques (2)*

- **Translation d'adresses : NAT/PAT**
- **DHCP Client, Serveur**
- **Firewall**
  - Filtrage, Inspection complète, Détection d'intrusion...
- **QoS IP (Diffserv) RFC 2475**
- **Configuration :**
  - Serveur HTTP intégré
  - Telnet
  - Configuration rapide
  - Mise à jour du firmware par FTP
  - Sauvegarde de la configuration



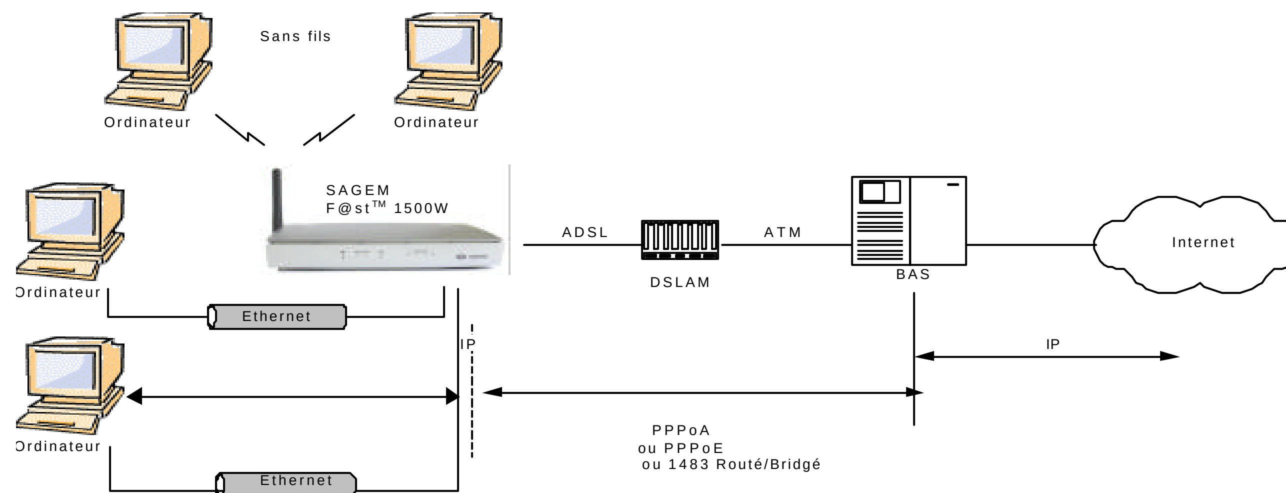
SAGEM F@st^{TM} 1500WG

- **Partage de l'accès Internet**
- **Wireless = sans fils**
- **Compatible avec les PC déjà installés :**
  - Ethernet + WIFI
- **Fonctions de sécurité intégrées :**
  - Wireless
  - Firewall
- **Solution complète**
  - Router ADSL sans fils + produits sans fil pour PC
- **Produit stylisé et compact**



SAGEM F@st™ 1500WG

Partager son accès Access

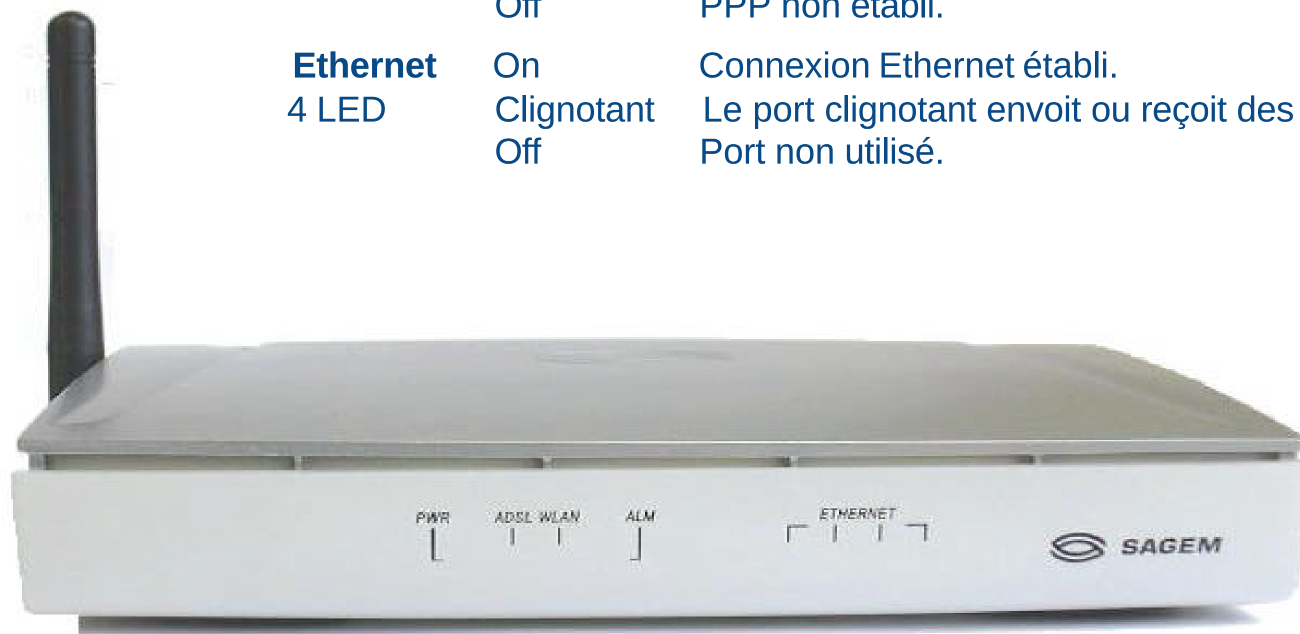


SAGEM F@st^{TM} 1500WG

- Généralités F@st 1500WG
- **Description physique**
- Installation du modem routeur
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP

Face avant

LED	Etat	Description
PWR	On Off	Le routeur est sous tension. Hors tension ou panne.
ADSL	On Clignotant Off	La connection ADSL fonctionne correctement. Le routeur ADSL est en cours de synchronisation. Connexion ADSL non établie.
WLAN	Clignotant	L' interface WIFI envoie ou reçoit des données.
ALM	On Off	PPP est établi. PPP non établi.
Ethernet 4 LED	On Clignotant Off	Connexion Ethernet établi. Le port clignotant envoit ou reçoit des données. Port non utilisé.



Face arrière

Port/Bouton	Description
ADSL	Port WAN (RJ-11). Connectez votre ligne ADSL à ce port.
Power	Branchez l'adaptateur secteur fourni sur cette prise. **Attention:** L'utilisation d'une alimentaion non adaptée peut endomager le routeur SAGEM F@st 1500.
Reset	Utilisez ce bouton pour redémarrer le routeur ou récupérer les paramètres par défaut. Pour redémarrer sans perdre la configuration, vous devez enregistrer vos paramètres.
I/O	Interrupteur marche/arrêt.
LAN 1-4	Connectez vos périphériques (ex: PC, hub ou switch) à ces ports Ethernet (RJ-45) pour accèder à votre réseau local.
Antenne	Antenne orientable (180°), non démontable. (seulement sur SAGEM F@st 1500WG).



SAGEM F@st™ 1500WG

- Généralités F@st 1500WG
- Description physique
- **Installation du modem routeur**
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP



Présentation fonctionnelle

- **Il faut distinguer les 2 réseaux :**
  - **WAN :** Réseau Internet, ligne supportant la transmission ADSLavec abonnement à un fournisseur de services, après configuration correcte des paramètres du fournisseur d'accès à Internet.
  - **LAN/ WLAN :** Réseau privé, terminaux (PC ou MAC) équipés d'une pile de protocoles TCP/IP et comportant une interface Ethernet (10Base-T ou 10/100Base-T) ou d'une interface WiFi (IEEE 802.11b/g).
- **1ère étape :** Reliez un PC au routeur afin de le configurer (vérifier la configuration IP de celui-ci).
- **2ème étape :** Configurez le routeur pour établir la liaison avec votre fournisseur d'accès.





Installation du routeur

- **Connexion du câble ADSL**
  - Utilisez le câble RJ11/RJ11 fourni avec le SAGEM F@st™ 1500WG.
  - Brancher le câble dans la prise marquée **LINE** à l'arrière du SAGEM F@st™ 1500WG.

- **Alimenter le routeur**
  - Vérifiez que le routeur SAGEM F@st™ 1500WG est correctement connecté à une prise secteur.
  - Mettre le bouton poussoir I/O en position I.

- **Utiliser une des interfaces :**
  - Interface Ethernet via un câble croisé ou droit
  - Interface sans fil via le dongle USB ou une carte PCMCIA
  - Hub/Switch sur Interface Ethernet

Connexion du PC au routeur

- Après avoir configuré TCP/IP sur votre PC, vous avez accès à la configuration du routeur SAGEM F@st 1500WG ADSL.

  Entrez l'adresse IP par défaut du routeur dans votre navigateur Internet : **192.168.2.1**

- Pour des raisons de sécurité, on peut interdire l'accès à la configuration du routeur par le WAN (défaut).
- L'écran de connexion suivant apparaît :
- Entrez le mot de passe et cliquez sur **Connecter**

  (le mot de passe par défaut est vide, dans ce cas, la fenêtre de connexion ne s'affiche pas).

Ecran de connexion

Mot de passe:

Connecter Annuler

SAGEM F@st^{TM} 1500WG

- Généralités F@st 1500WG
- Description physique
- Installation du modem routeur
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP

Sélection du pays

La première étape consiste à sélectionner le pays pour configurer votre point d'accès WiFi.

Sélectionner un pays dans la liste et cliquer sur le bouton **Appliquer**.

Vous devez sélectionner le pays en fonction de l'endroit ou vous utilisez votre point d'accès.

Exploiter votre point d'accès avec une configuration de pays incorrecte peut être illégal.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
Avancé

Sélection de pays

Veuillez sélectionner un pays afin de configurer le point d'accès pour votre emplacement :

Sélectionnez un pays...

Attention: Une fois que vous avez appliqué cette configuration, vous ne pouvez plus la modifier en reinitialisant le Point d'Accès avec ses valeurs de défauts.

Appliquer

Menu Configuration - Configuration de PPP

1. Configuration de PPP
2. Canal et SSID
3. WEP
4. Contrôle de l'accès

1. Configuration de PPP

Veuillez saisir votre nom d'utilisateur et votre mot de passe fournit par votre FAI.

Nom d'utilisateur	
Mot de passe	
Confirmer le mot de passe	

Suivant

Entrez les paramètres PPP fournis par votre fournisseur d'accès Internet.

Cliquer sur **Suivant**, le routeur va essayer de se connecter à Internet. Cela va automatiquement configurer le router SAGEM F@st 1500 avec le protocole, l'encapsulation et le couple VPI/VCI requis par votre fournisseur d'accès.

Le message suivant apparaît :

Connection à Internet en cours, veuillez patienter….

Puis :

Vous êtes connectés à Internet.

Cliquer sur **Suivant.**

Menu Configuration - Canal et SSID

Vous pouvez maintenant configurer l'interface sans fil.

Vous devez spécifier un canal radio et un SSID communs.
Ils seront utilisés par le routeur et tous ses clients.
Veillez à configurer tous les clients avec les mêmes paramètres. Puis, cliquer sur **Suivant**.

1. Configuration de PPP
2. Canal et SSID
3. WEP
4. Contrôle de l'accès

2. Canal et SSID

Cette page vous permet de définir un SSID et un ID du canal pour la connexion sans fil.
Dans un environnement sans fil, le routeur peut aussi faire office de point d'accès sans fil.
Ces paramètres sont utilisés pour la connexion des stations mobiles à ce point d'accès.

SSID	SAGEM
Diffusion SSID	Activer Désactiver
Mode sans fil	Mixte (11b+11g)
Canal	Auto

Précédent Suivant

SSID	Identifiant du point d'accès.
Diffusion SSID	Active ou désactive la diffusion du SSID.
Mode sans fils	Cet appareil supporte les normes 802.11g et 802.11b.
Canal	Canal radio utilisé par le routeur pour communiquer avec ses clients.

Menu Configuration - WEP

Pour sécuriser votre réseau sans fils, vous devez activer cette fonction.

Utilisez les mêmes paramètres sur le Router ADSL et tous ses clients sans fil.

Vous pouvez générer une clé automatiquement avec une **Phrase de passe**.
Notez que la fonction WEP protège les données transmises entre les noeuds, mais ne protège pas les transmissions entre votre réseau sans fils et Internet.

1. Configuration de PPP
2. Canal et SSID
3. WEP
4. Contrôle de l'accès

3. WEP

WEP est le mécanisme de base pour transmettre vos données en toute sécurité sur le réseau sans fil. Pour utiliser WEP, il faut définir des clés de cryptage compatibles sur votre routeur et vos appareils clients sans fil.

Activer ou désactiver la fonction du module WEP : Désactiver Activer

Mode WEP	64-bits 128-bits
Méthode de saisie des clés	Hexa ASCII

Définition de clé WEP statique

10/26 chiffres hexa pour 64-WEP/128-WEP

ID de clé par défaut	1
Phrase de passe	(1~32 caractères)
Clé 1	0101010101
Clé 2	0202020202
Clé 3	0303030303
Clé 4	0404040404
	Effacer

Précédent Suivant

Menu Configuration - Contrôle de l'accès

Le Contrôle de l'accès permet de configurer les clients autorisés à se connecter au point d'accès.

Ce menu vous permet de configurer 8 clients.

Le menu **Réseau sans fil** permet d'étendre la configuration à 32 clients.

Cliquer sur **Terminer**.

1. Configuration de PPP
2. Canal et SSID
3. WEP
4. Contrôle de l'accès

4. Contrôle de l'accès

Pour un réseau sans fil plus sûr, vous pouvez spécifier que seuls certains PC sans fil peuvent se connecter au point d'accès. Il est possible d'ajouter jusqu'à 8 adresses MAC à la Table de filtrage MAC. Quand le filtrage est activé, toutes les adresses MAC enregistrées sont contrôlées par la Règle d'accès.

- **Activer le filtrage MAC :** ○ Activer ◉ Désactiver
- **Règle d'accès pour les adresses MAC enregistrées :** ○ Autoriser ◉ Refuser
- **Table de filtrage MAC (jusqu'à 8 stations)**

ID	Adresse MAC
1	00 : 00 : 00 : 00 : 00 : 00
2	00 : 00 : 00 : 00 : 00 : 00
3	00 : 00 : 00 : 00 : 00 : 00
4	00 : 00 : 00 : 00 : 00 : 00
5	00 : 00 : 00 : 00 : 00 : 00
6	00 : 00 : 00 : 00 : 00 : 00
7	00 : 00 : 00 : 00 : 00 : 00
8	00 : 00 : 00 : 00 : 00 : 00

Ajouter les stations MAC actuellement associées

Précédent Terminer

Information (1)

Cet écran affiche le type de connexion WAN et son état, les paramètres IP du système, le nombre de clients DHCP, les numéros de version du matériel et du firmware, les tentatives illégales d'accès à votre réseau.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
Avancé

Information

ADSL

Etat	Mode actuel	Débit émission	Débit réception
ADSL: Connecté	MULTIMODE	160 Kb	608 Kb

Réseau Distant (WAN)

VC	Etat		VCC	Protocole	Nom d'utilisateur	Adr.IP publique
1	UP	Déconnecter	8/35/VC MUX	PPPoA	fti/6kwb77p	80.11.145.52/255.0.0.0, DNS1=80.10.246.130, DNS2=80.10.246.3

Réseau Local (LAN)/ Sans fil

Adr.IP locale	Masque de réseau	Serveur DHCP	WiFi	Canal WiFi	UPnP
192.168.2.1	255.255.255.0	Activé	Activé	6	Activé

Informations complémentaires

Version du firmware:	F@st 1500WG Ver. 2.0.12 (May 16 2005 10:25:20)
Version du code de démarrage:	0.62
Version du code du modem ADSL:	04.00.01.00A
Numéro de série:	A444039036
Version du matériel:	01
Adresse MAC LAN:	00-60-4C-68-DF-72
Adresse MAC sans fil:	00-60-4C-68-DF-74
Adresse MAC WAN:	00-60-4C-68-DF-73
Nombre de clients DHCP:	0

Information (2)

Le **Journal des connexions** permet de :

- Contrôler l'état du routeur,
- Visualiser les tentatives illégales d'accès.

Il peut être effacé ou sauvegardé en cliquant sur **Enregistrer** puis en choisissant le nom et la destination du fichier.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
Avancé

Journal des connexions

```
07/04/2005  14:39:58 sending ACK to 192.168.2.3
07/04/2005  14:39:56 sending OFFER to 192.168.2.3
07/04/2005  13:59:09 I/F(ATM1) PPP connection ok !
07/04/2005  13:59:08 ATM1 get IP:80.11.145.52
07/04/2005  13:59:02 ATM1 start PPP
07/04/2005  13:59:02 ADSL Media Up !
07/04/2005  13:47:31 I/F(ATM1) PPP connection ok !
07/04/2005  13:47:30 ATM1 get IP:80.11.145.32
07/04/2005  13:47:28 ATM1 start PPP
```

Enregistrer Effacer

Journal des clients DHCP

```
ip=192.168.2.3   mac=00-00-C0-6B-53-E9   name=fred
```


SAFRAN

Menu Système - Réglage de l'heure

Pour une gestion correcte de l'heure, événements système, filtrage des clients, vous devez sélectionner le bon fuseau horaire.

Le changement heure d'été / heure d'hiver n'est pas géré par le routeur, vous devez changer de fuseau horaire manuellement.

Information
Configuration
Système
» Réglage de l'heure
» Définition du mot de passe
» Outils de configuration
» Mise à jour du firmware
» Réinitialiser
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
Avancé

Réglage de l'heure

Définition du fuseau horaire:

Utilisez ce paramètre pour vous assurer que la fonction de filtrage des clients reposant sur l'heure et les entrées du journal système utilisent l'heure locale correcte.

(GMT+01:00)Brussels, Copenhagen, Paris, Vilnius

Configuration du serveur temporel (NTP) :

Vous pouvez maintenir automatiquement l'heure système sur votre routeur ADSL en effectuant une synchronisation avec un serveur temporel public sur Internet.

☑ Activation de la Maintenance automatique des serveurs temporels

Pour activer cette option, vous devez configurer deux serveurs temporels différents. Utilisez les options ci-dessous pour définir les serveurs NTP primaire et secondaire dans votre zone :

Serveur primaire: 129.132.2.21 - Europe

Serveur secondaire: 130.149.17.8 - Europe

Aide | Appliquer | Annuler

Menu Système - Définition du mot de passe

Utilisez cette page pour changer le mot de passe d'accès à l'interface de configuration du routeur.

Le mot de passe peut avoir entre 3 et 12 caractères alphanumeriques (minuscules et majuscules).

Si vous perdez le mot de passe, pressez le bouton **Reset** pendant plus de 5 secondes pour retrouver les paramètres par défaut. Le mot de passe par défaut est vide.

Le paramètre **Temps maximum d'inactivité** définit le temps maximum pendant lequel la session est maintenue sans activité.

Information
Configuration
Système
» Réglage de l'heure
» Définition du mot de passe
» Outils de configuration
» Mise à jour du firmware
» Réinitialiser
Réseau Distant
Réseau Local
Réseau Sans Fil

Définition du mot de passe

Vous définissez un mot de passe pour limiter l'accès à la gestion du routeur. Si vous souhaitez gérer le routeur depuis un emplacement distant (hors du réseau local), vous devez aussi spécifier l'adresse IP du PC distant. Vous pouvez le faire dans le menu Avancé – Gestion à distance.

- Mot de passe courant :
- Nouveau mot de passe:
- Retapez le mot de passe pour le vérifier:
- Temps maximum d'inactivité : 10 Min. (Temps d'inactivité = 0 : PAS de temps maximum)

Aide | Appliquer | Annuler

Menu Système - Outils de configuration

Utilisez le menu **Outils de configuration** pour :

- Sauvegarder la configuration courante du routeur
- Restaurer une configuration déjà sauvegardée
- Rétablir les paramètres par défaut du routeur

Choisissez une fonction et cliquez sur **Suivant**. Une confirmation vous sera demandée.

Information
Configuration
Système
» Réglage de l'heure
» Définition du mot de passe
» Outils de configuration
» Mise à jour du firmware
» Réinitialiser
Réseau Distant

Outils de configuration

Utilisez l'outil "Sauvegarder" pour sauvegarder la configuration courante du routeur dans un fichier appelé "backup.bin" sur votre PC.
Vous pouvez utiliser l'outil "Restaurer" pour rétablir la configuration enregistrée du routeur.
Sinon, vous pouvez utiliser l'outil "Restaurer les paramètres par défaut" pour forcer le routeur à effectuer une réinitialisation d'alimentation et restaurer les paramètres définis en usine.

- (•) Sauvegarder la configuration du routeur
- ( ) Restaurer en utilisant le fichier de configuration sauvegardé (backup.bin)
- ( ) Rétablir les paramètres par défaut du routeur

Suivant >>

Menu Système - Mise à jour du firmware et Réinitialisation

Information
Configuration
Système
» Réglage de l'heure
» Définition du mot de passe
» Outils de configuration
» Mise à jour du firmware
» Réinitialiser
Réseau Distant

Mise à jour du firmware

Cet outil vous permet de mettre à jour le firmware du routeur à l'aide d'un fichier que nous fournissons. Vous pouvez télécharger le firmware le plus récent depuis le site http://www.sagem.com

Entrez le chemin et le nom du fichier de mise à niveau ou naviguez jusqu'à son emplacement puis cliquez sur le bouton "Appliquer". Le système vous demandera de confirmer la mise à jour avant de procéder à l'opération.

Fichier de firmware [ ] Parcourir...

Aide | Appliquer | Annuler

Information
Configuration
Système
» Réglage de l'heure
» Définition du mot de passe
» Outils de configuration
» Mise à jour du firmware
» Réinitialiser

Réinitialiser

Si le système ne répond plus correctement ou si d'une manière ou d'une autre il s'arrête de fonctionner, vous pouvez faire une réinitialisation. Vos paramètres restent inchangés. Pour faire une réinitialisation, cliquez sur le bouton "Appliquer" ci-dessous. Le système vous demandera de confirmer votre décision. La réinitialisation sera terminée quand le voyant d'alimentation cessera de clignoter.

Aide | Appliquer | Annuler

Menu Réseau Distant

Le routeur ADSL utilise ATM comme protocole de niveau 2.

Le PVC ATM est une connexion virtuelle qui fait office d'interface WAN.

Cette page permet d'accéder à la configuratio des 8 PVC ATM supportés par le routeur.

Information
Configuration
Système
Réseau Distant
» VC1
» VC2
» VC3
» VC4
» VC5
» VC6
» VC7
» VC8
» MAC Adresse

Réseau Distant (WAN)

Le router peut se connecter à votre fournisseur d'accès par une des méthodes suivantes

PVC ATM Pour configurer les paramètres VC ATM
Gestion de MAC Adresse Pour configurer l'adresse MAC de l'interface WAN

Information
Configuration
Système
Réseau Distant
» VC1
» VC2
» VC3
» VC4
» VC5
» VC6
» VC7
» VC8
» MAC Adresse

PVC ATM

Le routeur ADSL utilise ATM comme protocole de niveau 2. Le PVC ATM est une connexion virtuelle qui fait office d'interface WAN. La Passerelle peut prendre en charge jusqu'à 8 PVC ATM.

Description	VPI/VCI	Encapsulation	Protocole
VC1	8/35	VC MUX	PPPoA
VC2	-/-	---	---
VC3	-/-	---	---
VC4	-/-	---	---
VC5	-/-	---	---
VC6	-/-	---	---
VC7	-/-	---	---
VC8	-/-	---	---

Menu Réseau Distant - Interface ATM

Information
Configuration
Système
Réseau Distant
» VC1
» VC2
» VC3
» VC4
» VC5
» VC6
» VC7
» VC8
» MAC Adresse
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS

Interface ATM

	ATM1
Protocole	PPPoA
VPI/VCI	8 / 35
Encapsulation	VC MUX
Classe de QoS	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP attribué par le FAI	Yes
Adresse IP	0.0.0.0
Masque de sous-réseau	0.0.0.0
Type de connexion	Toujours connecté
Temps d'inactivité (minutes)	20
Nom d'utilisateur	fti/6kwb77p
Mot de passe	●●●●●●●
Confirmer le mot de passe	●●●●●●●
MTU	1500

- **Protocole :** Disable, 1483 Bridging, PPPoA, 1483 Routing, PPPoE, MAC Encaps Routing
- Virtual Path Identifier et Virtual Circuit Identifier
- **Encapsulation :** LLC et VCMUX sont supportés
- **Classe de QoS :** CBR, UBR et VBR
- Paramètres QoS : Peak Cell Rate, Sustainable Cell Rate et Maximum Burst Size sont configurables

- Adresse IP et masque de l'interface ATM

- Toujours connecté, Auto (déclanché par le trafic) ou manuel

- Maximum Transmit Unit

Menu Réseau Distant - MAC Adresse

Cette fonction permet de modifier l'adresse MAC WAN du routeur si votre fournisseur d'accès le désire.
Tous les PVC ATM avec encapsulation Ethernet utilisent la même adresse MAC.

Information
Configuration
Système
Réseau Distant
» VC1
» VC2
» VC3
» VC4
» VC5
» VC6
» VC7
» VC8
» MAC Adresse

Gestion de MAC Adresse

Certains FAI pourrait vous demander de enregistrer votre MAC addresse avec eux. Si vous faites cette manipulation, le passerell MAC adresse doit être assigné à celle fournie par votre FAI.

- Interface WAN MAC Adresse:

◉ Utiliser le défault MAC adresse de passerelle. **00:60:4C:68:DF:73**

○ Utiliser Le MAC adresse de votre ordinateur. **00:00:C0:6B:53:E9**

○ Donner une nouvelle MAC adresse manuallement:

00 : 00 : C0 : 6B : 53 : E9

Aide | Appliquer | Annuler

Menu Réseau Local

Vous pouvez activer le serveur DHCP pour attribuer dynamiquement des adresses IP aux PC clients.

L'adresse IP du routeur doit être dans le même réseau que le pool d'adresses IP.

Durée du bail : Période pendant laquelle le DHCP fournira la même adresse IP pour la même adresse MAC.

Information
Configuration
Système
Réseau Distant
Réseau Local
» VLAN
» DNS
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
Avancé

IP LAN

Adresse IP	192.168.2.1
Masque de sous-réseau	255.255.255.0
Serveur DHCP	Activer Désactiver

VLAN Binding

LAN1	Default
LAN2	Default
LAN3	Default
LAN4	Default
WLAN	Default

Durée du bail	Deux jours

Pool d'adresses IP

IP de départ	192.168.2.2
IP de fin	192.168.2.254
Nom de domaine	

Menu Réseau Local - VLAN (LAN Virtuel)

Les **VLAN** sont organisés et contrôlés par des profils VLAN.

Vous pouvez créer jusqu'à 5 profils VLAN.

Dès qu'un profil est créé, il est vide et l'utilisateur peut lui associer des interfaces.

Seuls les ports LAN et les PVC 1483 bridged peuvent être associés à un VLAN.

Le VLAN par défaut peut être modifié mais vous ne pouvez pas le supprimer.

Le serveur DHCP est attaché au VLAN par défaut. Les 4 autres VLAN utilisent un plan d'adressage IP statique.

Pour créer un profil VLAN, cliquez sur **Ajouter un VLAN**.

Utilisez les boutons **Modifier** et **Supprimer** pour modifier et supprimer un profil.

Information
Configuration
Système
Réseau Distant
Réseau Local
» VLAN
» DNS
Réseau Sans Fil

Profil VLAN

- table VLAN (5 profils max)

Num.	VLAN	Interfaces groupées	Configurer
1	Default	LAN1,LAN2,LAN3,LAN4,WLAN	Modifier

Ajouter un VLAN

Aide Annuler



Menu Réseau Local - ADD VLAN

Domaine NAT - Le domaine d'adressage NAT permet de définir le mode NAPT de l'interface virtuel VLAN. Il y a 2 options pour le domaine NAT : privé et publique. Le mode NAPT est seulement appliqué aux les flux entre différents domaines NAT. Car toutes les interfaces/connexions WAN (ex. ATM PVC) sont configurés statiquement dans le domaine public NAT, le VLAN dans le domaine public NAT sera considéré comme dans un domaine public d'adressage IP et aucun mode NAPT ne sera appliqué aux flux entre les interfaces VLAN et WAN. Par contre, le VLAN dans le domaine privé NAT est comme un réseau privé et tous les flux se feront passer pour du réseau privé entre les interfaces VLAN et WAN.

IGMP Snooping - Activer/désactiver ce mécanisme pour bloquer l'inondation inutile de trafic IP en multidiffusion sur les ports VLAN sans adhésion en multidiffusion. Ce mécanisme se base sur des messages de type IGMP snooping (Joindre/Quitter le groupe de multidiffusion) sur les ports VLAN pour mettre à jour la base de données de la table d'acheminement. Le mécanisme IGMP snooping est extrémement utile en préservant la bande passante des interfaces moins rapides (ex. WLAN) d'améliorer l'utilisation du réseau.

IGMP Querier - Activer/Désactiver le mécanisme de requêtes de participants IGMP en multidiffusion sur les interfaces virtuelles VLAN. L'option permet de contrôler si le mécanisme des requêtes de participants IGMP en multidiffusion est activé sur le réseau VLAN. Si le mécanisme des requêtes de participants IGMP est désactivé, le routeur va réagir comme une station en multidiffusion IP et envoyer des rapports de participants IGMP pour ses propres groupes abonnés en multidiffusion IP. Aucun message de requête de participant IGMP en multidiffusion ne sera envoyé sur le VLAN spécifique correspondant.

Information
Configuration
Système
Réseau Distant
Réseau Local
» VLAN
» DNS
Réseau Sans Fil

Paramètres VLAN

Entrez les parametres du profil VLAN.

Description	Réseau_1
Adresse IP	10 . 10 . 1 . 1
Masque de sous-réseau	255 . 255 . 255 . 0
Domaine NAT	(•) Privé ( ) Public
IGMP Snooping	( ) Activer (•) Désactiver
IGMP Querier	( ) Activer (•) Désactiver

Menu Réseau Local - ADD VLAN

Après avoir créé un VLAN (ex: Réseau_1), vous pouvez l'utiliser pour relier cette interface ATM un port physique du routeur.

Seul le protocole RFC 1483 bridgé vous le permet.

] Sélectionnez le VLAN que vous venez de créer dans le menu **Réseau Distant**.

Interface ATM

	ATM2
Protocole	RFC 1483 bridgé
VLAN	Réseau_1
VPI/VCI	0 / 0
Encapsulation	VC MUX
Classe de QoS	UBR
PCR/SCR/MBS	4000 / 4000 / 10

] Dans le menu **Réseau local**, affectez votre nouveau réseau au port physique (LAN3 dans cet exemple).

VLAN Binding

LAN1	Default
LAN2	Default
LAN3	Réseau_1
LAN4	Default
WLAN	Default

Menu Réseau Local - DNS (Domain Name Server)

Le DNS (Domain Name Server) est utilisé pour remplacer un nom de domaine par son adresse IP.

Les DNS fournis par votre FAI apparaissent dans la page **Information**.

Cependant, vous pouvez en utiliser d'autres et les configurer dans cette page.

Puis, cliquez sur **Appliquer**.

Menu Réseau Sans Fil (Wireless)

Le routeur ADSL SAGEM F@st 1500WG peut être utilisé comme point d'accès sans fil.

Pour activer cette fonction, vous devez :

- Activer la fonction dans cette page,
- Configurer le nom du point d'accès (SSID),
- Choisir un numéro du canal,
- Activer le cryptage des données pour sécuriser le réseau.

Cliquer sur **Activer** puis sur **Appliquer**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
» Canal et SSID

Réseau Sans Fil (Wireless)

La passerelle peut être rapidement configurée comme point d'accès sans fil pour les clients itinérants en définissant l'identificateur de services (SSID) et le numéro du canal. Elle gère également le cryptage des données et le filtrage des clients.

Activer ou désactiver la fonction du module Sans fil : Activer Désactiver

Aide Appliquer Annuler

Menu Réseau Sans Fil - Canal et SSID

Cette page vous permet de définir le canal radio et le SSID pour les connexions sans fil.
Veillez à configurer tous les clients avec les mêmes paramètres.
Puis cliquer sur **Appliquer**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
» Canal et SSID
» Contrôle de l'accès
» Sécurité
» Clés WEP
» Clés WPA
» 802.1X

Canal et SSID

Cette page vous permet de définir le SSID et l'ID du canal pour la connexion sans fil. Dans l'environnement sans fil, cette passerelle peut aussi faire office de point d'accès sans fil. Ces paramètres sont utilisés pour la connexion des stations mobiles à ce point d'accès.

SSID	SAGEM
Diffusion SSID	Activer / Désactiver
Mode sans fil	Mixte (11b+11g)
Canal	Auto

Aide | Appliquer | Annuler

SSID Service Set ID (doit être le même sur le routeur et tous les clients).
Diffusion SSID Active ou désactive la diffusion du SSID.
Mode sans fil Ce routeur supporte les normes 802.11g et 802.11b.
Canal Canal radio utilisé par le routeur pour communiquer avec tous les clients (doit être le même sur le routeur et tous les clients).

Menu Réseau Sans Fil - Contrôle de l'accès

Cette fonction permet de contrôler l'accès au point d'accès depuis les clients sans fil en fonction de leur adresse MAC. Vous pouvez **Autoriser** ou **Refuse**r tous les clients configurés dans cette page.

ID	Adresse MAC
1	00 : 00 : 00 : 00 : 00 : 00
2	00 : 00 : 00 : 00 : 00 : 00
3	00 : 00 : 00 : 00 : 00 : 00
4	00 : 00 : 00 : 00 : 00 : 00
5	00 : 00 : 00 : 00 : 00 : 00
6	00 : 00 : 00 : 00 : 00 : 00
30	00 : 00 : 00 : 00 : 00 : 00
31	00 : 00 : 00 : 00 : 00 : 00
32	00 : 00 : 00 : 00 : 00 : 00

Menu Réseau Sans Fil - Sécurité

Pour sécuriser votre réseau sans fil, vous devez activer une des fonctions supportées :

Le routeur ADSL SAGEM F@st 1500WG supporte:

- WEP (Wired Equivalent Privacy) 64 ou 128 bits,
- WPA (Wi-Fi Protected Access),
- Authentification 802.1x.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
» Canal et SSID
» Contrôle de l'accès
» Sécurité
» Clés WEP
» Clés WPA

Sécurité

Le routeur peut transmettre vos données en toute sécurité sur le réseau sans fil.
Il faut définir des mécanismes de sécurité compatibles sur votre routeur et vos appareils clients sans fil.
Vous pouvez choisir les mécanismes de sécurité autorisés dans cette page et les configurer dans les sous-pages.

Le sécurité type supporté : Ni WEP, ni WPA

Ni WEP, ni WPA
Uniquement WEP
Uniquement WPA

Aide | Appliquer | Annuler

Menu Réseau Sans Fil - Clés WEP

Vous pouvez générer automatiquement les clés de cryptage avec une **Phrase de passe** ou les saisir manuellement.

Si vous voulez attribuer les clés dynamiquement, vous devez d'abord activer la fonction 802.1x (pour celà, un serveur Radius est nécessaire).



Menu Réseau Sans Fil - Clés WPA (Wi-Fi Protect Access)

WPA combine le protocole **TKIP** (Temporal Key Integrity Protocol) et l'authentification **802.1x**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
» Canal et SSID
» Contrôle de l'accès
» Sécurité
» Clés WEP
» Clés WPA
» 802.1X
Nat

Clés WPA

WPA est une option de sécurité permettant de renforcer considérablement le niveau de protection des données et le contrôle d'accès pour le LAN sans fil existant. Pour utiliser WPA, il faut définir des méthodes d'authentification et de cryptage compatibles sur votre routeur et vos appareils clients sans fil.

Cypher suite	TKIP
Authentication	○ 802.1X ◉ Clé prépartagée
Type de clé prépartagée	◉ Phrase de passe (8~63 caractères) ○ Hexa (64 chiffres)
Clé prépartagée	
Recomposition de la clé de groupe	◉ Per 86400 Secondes ○ Per 1000 Paquets de K ○ Désactiver

Cypher suite	Mécanisme de sécurité utilisé (actuellement, seul TKIP est supporté).	
Authentification	**802.1x**	pour les réseaux d'entreprise avec un serveur RADIUS.
	Clé prépartagée	sans serveur d'authentification.
Type de clé prépartagée	Sélectionner la clé à utiliser.	
Clé prépartagée	Saisir la clé dans ce champ.	
Recomposition de la Clé de groupe	Période de renouvellement de la clé broadcast/multicast.	

Menu Réseau Sans Fil - 802.1x (1)

Cette page permet d'activer l'authentification 802.1x si vous avez un serveur RADIUS.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
» Canal et SSID
» Contrôle de l'accès
» Sécurité
» Clés WEP
» Clés WPA
» 802.1X
Nat
Pare-Feu
Routage
QoS
Avancé

802.1X

Cette page vous permet de définir le 802.1X, une méthode d'authentification pour les connexions sans fil. Ces paramètres sont utilisés pour la connexion de ce point d'accès au serveur d'authentification.

Authentification 802.1X	○ Activer ◉ Désactiver
Temps maximum d'inactivité d'une session	300 Secondes (0 pour aucun contrôle du temps maximum)
Période de ré-authentification	3600 Secondes (0 pour aucune ré-authentification)
Période calme	60 secondes après l'échec de l'authentification
Type de serveur	RADIUS

Paramètres du serveur RADIUS

IP du serveur	192 . 168 . 2 . 1
Port du serveur	1812
Clé secrète	
NAS-ID	

Menu Réseau Sans Fil - 802.1x (2)

802.1x

Authentification 802.1x	Active ou désactive cette fonction.
Temps max d'inactivité d'une session	Durée (en secondes) pendant laquelle la connexion est maintenue sans activité.
Période de Ré-authentification	Période au delà de laquelle le client devra se ré-authentifier.
Période calme	Période d'attente (en secondes) de la passerelle entre des authentifications échouées.
Type de Serveur	Type de serveur d'authentication (TINY non supporté).

Paramètres du Serveur RADIUS

IP du serveur	Adresse IP de votre server RADIUS.
Port du serveur	Port utilisé par le serveur d'authentification.
Clé secrète	Clé d'authentification secrète utilisée par le serveur et ses clients.
NAS-ID	Identifiant du Serveur d'Accès Réseau.

SAGEM F@st™ 1500WG

- Généralités F@st 1500WG
- Description physique
- Installation du modem routeur
- Configuration du modem routeur
- **Installation des modules Wi-Fi**
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP

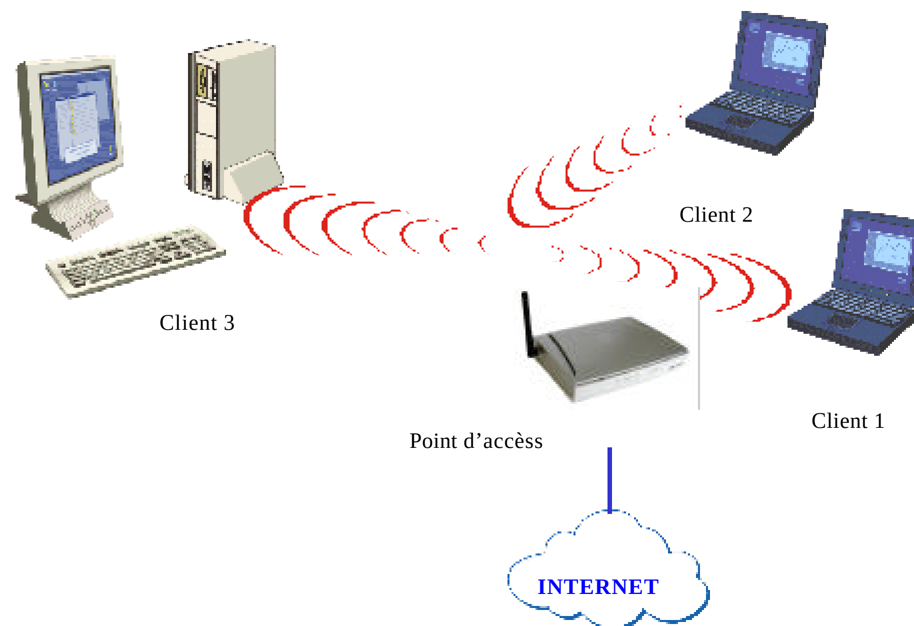
Installation des modules WiFi

L'adaptateur USB pour réseau sans fil est une carte réseau fonctionnant avec des vitesses de 54, 11, 5.5, 2 ou 1 Mbps en utilisant la bande des 2.4 GHz.

Le mode de transmission supporté est DSSS (Direct Sequence Spread Spectrum), transmission implementée dans la norme IEEE 802.11b/g.

Son port USB est compatible USB 1.1.

Les adaptateurs réseaux sans fil sont compatibles Windows 98SE/ME/2000/XP.



SAFRAN



Installation des modules WiFi

L 'installation de votre adaptateur Wi-Fi demande 3 étapes: **-** Installation du driver
- Installation du matériel
- Configuration des connexions sans fil

<u>1ere étape</u> : Copie sur votre disque dur des fichiers correspondants à votre nouvel équipement. Pour cela, insérez le CD-ROM dans votre lecteur et suivez les instructions.

.

<u>2ème étape :</u> Enlevez le capot de protection du connecteur USB de votre adaptateur Wi-Fi. Insérez le connecteur USB de votre adaptateur dans le port USB de votre PC. Windows doit détecter automatiquement le nouveau périphérique, et exécuter l'assistant d'ajout d'un nouveau matériel.

Sous Windows XP, un écran apparaît :

Sélectionnez **Installer le logiciel automatiquement (Recommandé)**, puis cliquez sur **Suivant** pour continuer.

Note: Cet écran n'apparaît pas sous Windows 98SE, ME et 2000. Le processus se poursuit automatiquement.

<u>3éme étape</u> : Configuration de votre adaptateur USB Wi-Fi.

- Lancez l'utilitaire de gestion du réseau sans fil,
- Configurez votre adaptateur USB Wi-Fi en mode Infrastructure,
- Précisez le nom de réseau sans fil (SSID) auquel vous souhaitez vous attacher,
- Configurez les paramètres de cryptage.

Supervision de l 'adaptateur USB Wi-Fi

Etat :	Ce champ indique l 'adresse MAC du point d 'accès (mode infrastructure) ou de la station distante (mode Ad-Hoc) en connexion radio
Canal utilisé :	Indique le canal radio utilisé par la connexion en cours.
Vitesse d'émission :	Indique le débit maximum de la connexion en cours 11 Mbps, 5.5 Mbps, 2 Mbps or 1 Mbps.
Débits :	Indique les débits instantanés en émission et réception (en octets/secondes). Ces débits sont actualisés en permanence.
Qualité de la liaison :	Celle-ci dépend de la qualité du signal reçu.
Intensité du signal :	Celle-ci dépend de l'intensité du signal reçu.

Default - Sagem 802.11b PCMCIA

État | Configuration | Cryptage | À propos de

État : Associé:TestWifi - 00:60:B3:6B:74:DB

Vitesse d'émission : 1 Mb/s

Voie de transmission : 6 — Nouveau balayage — Désactiver radio

Débit (octets/s) : Transmission : 28 — Réception : 564

Qualité de la liaison : Excellente

Intensité du signal : Excellente

OK — Annuler — Appliquer

Etat

Etat : <Infrastructure> - TestWifi - 00:60:B3:6B:74:DB

Canal utilisé : 6 — Vitesse d'émission utilisée : 11 Mbit/s

Débit (octet/s) : TX : 0 — RX : 0

Qualité de la liaison : Excellente(100%)

Intensité du signal : Excellente(100%) — Nouveau balayage

Sagem - Utilitaire pour Clé Wi-Fi USB 802.11b

Configuration | Info IP | Détecteur d'AP | A propos de

Profil : <Infra> "TestWifi" — Sauvegarder — Supprimer

Configuration

SSID : TestWifi — Avancé

Type de réseau : Infrastructure — WEP Validé — clé WEP

Voie AdHoc : 6

Vitesse d'émission : Auto — Par défaut — Appliquer

Etat

Etat : <Infrastructure> - TestWifi - 00:60:B3:6B:74:DB

Canal utilisé : 6 — Vitesse d'émission utilisée : 11 Mbit/s

Débit (octet/s) : TX : 245 — RX : 0

Qualité de la liaison : Excellente(100%)

Intensité du signal : Excellente(100%) — Nouveau balayage

SAGEM F@st™ 1500WG

- Généralités F@st 1500WG
- Description physique
- Installation du modem routeur
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP



Menu NAT

Le mécanisme de **translation d'adresses** (**N**etwork **A**ddress **T**ranslation) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4.

Le **NAT statique** consiste à associer une adresse IP publique à une adresse IP privée.
Le routeur permet d'associer à une adresse IP privée (par exemple *192.168.1.2*) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

Le **NAT dynamique** permet de partager une (ou plusieurs) adresse(s) IP routable(s) entre plusieurs machines en adressage privé. Ainsi toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.

Afin de pouvoir multiplexer les différentes adresses IP privées sur une ou plusieurs adresses IP routables, le NAT dynamique utilise la translation de port (**PAT** - **P**ort **A**ddress **T**ranslation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

Cliquez sur **Activer** puis sur **Appliquer**.

Réseau Sans Fil
Nat
» Mappage des adresses
» Serveur virtuel
» Application spéciale
» Table de mappage Nat
Pare-Feu

Nat

Le Nat (Network Address Translation) permet à plusieurs utilisateurs de votre site local d'accéder à Internet avec une seule adresse IP publique ou plusieurs adresses IP publiques. Nat peut aussi empêcher les attaques de pirates en mappant les adresses locales à des adresses publiques pour les services clés tels que le Web ou FTP.

Activer ou désactiver la fonction du module Nat : ◉ Activer ○ Désactiver

Aide | Appliquer | Annuler

Menu NAT - Mappage des adresses

Cette fonction est utile si un utilisateur possède plusieurs adresses IP publiques.

Elle permet de répartir les utilisateurs locaux en plusieurs groupes.

Le routeur ADSL SAGEM F@st 1500WG peut supporter jusqu'à 10 adresses IP publiques.

Entrez l'adresse IP Publique que vous voulez partager dans le champ **IP global**.

Entrez le pool d'adresses IP qui partageront l'IP global, puis cliquez sur **Appliquer**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
» Mappage des adresses
» Serveur virtuel
» Application spéciale
» Table de mappage Nat
Pare-Feu
Routage
QoS

Mappage des adresses

Avec le Nat (Network Address Translation), les adresses IP utilisées dans un réseau local privé peuvent être mappées à une ou plusieurs adresses utilisées dans l'Internet public. Cette fonctionnalité limite le nombre d'adresses IP publiques requises du FAI et assure également la confidentialité et la sécurité du réseau local. Nous permettons le mappage de une ou plusieurs adresses IP publiques à un pool d'adresses locales.

Mappage des adresses

1. IP global: 80.110.120.11 est transformé en adresses IP virtuelles multiples
de 192.168.2.2 à 192.168.2.100

2. IP global: 80.110.120.12 est transformé en adresses IP virtuelles multiples
de 192.168.2.101 à 192.168.2.250

3. IP global: est transformé en adresses IP virtuelles multiples
de à

Menu NAT - Serveur virtuel

Cette fonction permet à des utilisateurs distants d'accèder à des serveurs de votre réseau privé (ex: serveur WEB ou FTP …) via votre adresse IP publique.
Nous vous conseillons de configurer vos serveurs locaux avec des adresses IP fixes.

Le routeur SAGEM F@st 1500WG permet de configurer 20 serveurs locaux. Vous pouvez utiliser une plage de ports (80-90), plusieurs ports (25, 35) et la combination des deux (40-50, 70).

Pour utiliser des logiciels **Peer to Peer** comme Winmx (port 4699) ou eMule/eDonkey (ports 4662 TCP et 4672 UDP), cette configuration est obligatoire.

Si vous voulez utiliser le même serveur sur plusieurs PC, vous devez changer les ports par défaut.

Une liste de ports standardisés est disponible à cette adresse : http://www.iana.org/assignments/port-numbers.

L'exemple suivant utilise un serveur FTP, Winmx et Emule.

Cochez la case **Activer**, puis cliquez sur **Ajouter**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
» Mappage des adresses
» Serveur virtuel
» Application spéciale
» Table de mappage Nat

Serveur virtuel

Num.	Adresse IP LAN	Type de protocole	Port LAN	Port Public	Activer	
1	192.168.2.10	☑ TCP ☑ UDP	21 20	21 20	☑	Ajouter Effacer
2	192.168.2.20	☑ TCP ☑ UDP	4662 4672	4662 4672	☑	Ajouter Effacer
3	192.168.2.20	☑ TCP ☐ UDP	4699	4699	☑	Ajouter Effacer
4		☐ TCP ☐ UDP			☐	Ajouter Effacer

Menu NAT - Application spéciale

Certaines applications nécessitent plusieurs connexions. Ces applications ne peuvent ne pas fonctionner quand le **NAT** est activé. Spécifiez le port normalement associé à une application dans le champ **Port de déclenchement**, sélectionnez le type de protocole puis entrez les ports publics associés au port de déclenchement pour les ouvrir au trafic entrant. La plage des ports de déclanchement va de 1 à 65535.

Cette page permet de configurer jusqu'à 10 applications spéciales.

Vous pouvez utiliser la configuration préparée pour quelques applications populaires.
Pour celà, sélectionnez l'application dans le champ puis cliquer sur **Copier dans** après avoir choisi le numéro de la ligne.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
» Mappage des adresses
» Serveur virtuel
» Application spéciale
» Table de mappage Nat
Pare-Feu
Routage
QoS
Avancé

Application spéciale

	Port de déclenchement	Type de déclenchement	Port public	Type public	Activé
1.	28800	TCP / UDP (UDP)	6667,2300-2400,47624,28800-29000	TCP (TCP) / UDP	☑
2.	2019	TCP (TCP) / UDP	2000-2038,2050-2051,2069,2085,3010-303	TCP (TCP) / UDP	☑
10.		TCP (TCP) / UDP		TCP (TCP) / UDP	☐

Popular applications: – séléctionner une parmie les suivantes – | COPIER DANS | 2

– séléctionner une parmie les suivantes –
Battle.net
Dialpad
ICU II
MSN Gaming Zone
PC-to-Phone
Quick Time4

Aide | Appliquer | Annuler

Menu NAT - Table de mappage NAT

La Table de mappage NAT affiche les mappages d'adresses NAPT courants.

IP local	Adresse IP de l'hôte local (LAN) pour le flux
Port local	Numéro du port de l'hôte local (LAN) pour le flux
Pseudo IP	Adresse IP convertie pour le flux
Pseudo port	Numéro de port converti pour le flux
IP point à point	Adresse IP de l'hôte distant (WAN) pour le flux
Port point à point	Numéro du port de l'hôte distant (WAN) pour le flux

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
» Mappage des adresses
» Serveur virtuel
» Application spéciale
» Table de mappage Nat
Pare-Feu
Routage
QoS
Avancé

Table de mappage Nat

Index	Protocole	IP Local	Port Local	Pseudo IP	Pseudo Port	IP point à point	Port point à point
1	TCP	192.168.2.3	4475	80.11.145.45	4475	62.23.137.34	80
2	TCP	192.168.2.3	4425	80.11.145.45	4425	62.23.137.34	80
3	TCP	192.168.2.3	4427	80.11.145.45	4427	62.23.137.170	80
4	TCP	192.168.2.3	4482	80.11.145.45	4482	62.23.137.34	80
5	TCP	192.168.2.3	4483	80.11.145.45	4483	62.23.137.34	80
6	TCP	192.168.2.3	4522	80.11.145.45	4522	82.227.30.110	5300
7	TCP	192.168.2.3	4542	80.11.145.45	4542	212.27.40.252	21
8	TCP	192.168.2.3	4443	80.11.145.45	4443	81.52.201.78	80
9	UDP	192.168.2.3	123	80.11.145.45	56400	207.46.130.100	123

Page: 1/1

|<< >>| Actualiser Aide

Menu Pare-Feu

Le pare-feu du routeur ADSL SAGEM F@st 1500WG permet :

- Le contrôle d'accès en définissant les applications autorisées pour chaque utilisateur,
- Le filtrage MAC,
- Le blocage d'URL ou mots clés,
- Des règles d'horaires,
- La détection d'intrusions SPI (Stateful Packet Inspection) et Anti-DoS,
- La création d'un zone Démilitarisée (DMZ)

Pare-Feu
» Contrôle de l'accès
» Filtre Mac
» Blocage d'URL
» Réglage de l'horaire
» Détection des intrusions
» DMZ
Routage

Pare-Feu (Firewall)

L'appareil assure une protection robuste de type pare-feu en forçant les paramètres de connexion à limiter le risque d'attaques de pirates et en protégeant contre un vaste éventail d'attaques courantes. Cependant, pour les applications qui nécessitent un accès non restreint à Internet, vous pouvez configurer un client/serveur spécifique comme une zone démilitarisée (DMZ).

Activer ou désactiver les fonctions de pare-feu : ⦿ Activer ○ Désactiver

Aide | Appliquer | Annuler

Menu Pare-Feu - Contrôle de l'accès

Le contrôle de l'accès permet de définir le trafic sortant permis ou non pour l'interface WAN.

L'option par défaut consiste à autoriser tout le trafic sortant.

Pour ajouter un PC dans la table de filtrage :

- Cliquer sur **Ajouter un PC** dans la page **Contrôle de l'accès**,
- Définissez la configuration appropriée pour un PC (ou une plage d'adresses IP),
- Cliquez sur **OK** puis sur **Appliquer**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
» Contrôle de l'accès
» Filtre Mac
» Blocage d'URL
» Réglage de l'horaire
» Détection des intrusions
» DMZ
Routage

Contrôle de l'accès

- Activer la fonction de filtrage : Activer Désactiver
- Inbound Default Rules :

Activer	Service
☑	RIP (UDP 520)
☑	BOOTP (UDP 67)

- Table de filtrage normal (jusqu'à 10 ordinateurs)

Description du PC client	Adresse IP du PC client	Service au client	Réglage de l'horaire	Configurer
Test	192.168.2.10 ~ 20	Telnet	Toujours Bloqué	Modifier Supprimer

Ajouter un PC

Aide Appliquer Annuler



Menu Pare-Feu - Contrôle de l'accès - Ajouter un PC

Cette page permet de définir des restrictions d'accès au WAN pour les PC clients, notamment, le type de service, des plages de ports et des règles d'horaire.

Pour la fonction **Blocage d'URL**, vous devez d'abord configurer les sites interdits.

Pour la fonction **Réglage d'horaire**, vous devez d'abord configurer la page **Réglage de l'horaire**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
» Contrôle de l'accès
» Filtre Mac
» Blocage d'URL
» Réglage de l'horaire
» Détection des intrusions
» DMZ
Routage
QoS
Avancé

Contrôle de l'accès Ajouter un PC

- Déscription du PC client:
- Adresse IP du PC client: ~
- Service au client:

Nom de Service	Déscription détaillée	Bloqué
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	☐
WWW avec bloquage de URL	HTTP (voir Bloquage de URL et Page Site)	☐
Envoy d'E-mail	SMTP, TCP Port 25	☐
Forums de News	NNTP, TCP Port 119	☐
Réception d'E-mail	POP3, TCP Port 110	☐
HTTP Sécurisé	HTTPS, TCP Port 443	☐
Transfert de Fichier	FTP, TCP Port 21	☐
Service Telnet	TCP Port 23	☐
AIM	AOL Instant Messenger, TCP Port 5190	☐
NetMeeting	H.323, TCP Port 1720, 1503	☐
DNS	UDP Port 53	☐
SNMP	UDP Port 161, 162	☐
VPN-PPTP	TCP Port 1723	☐
VPN-L2TP	UDP Port 1701	☐
TCP	Tous les Ports TCP	☐
UDP	All UDP Port	☐

Service Définie par Utilisateur.
Protocol: ○ TCP ○ UDP
Plage de port: 0 ~ 0 , 0 ~ 0 , 0 ~ 0 , 0 ~ 0 , 0 ~ 0
Effacer

- Réglage d'Horaire: Toujours Bloqué
  Toujours Bloqué
  8h–18h
  Total mercredi

OK Annuler

SAFRAN

Menu Pare-Feu - Filter MAC

Quand cette table est activée, seules les adresses MAC configurées ont accès à votre réseau.

Tous les autres clients auront leur accès refusé.

Cette fonction peut gérer jusqu'à 32 PC.

Vous pouvez saisir l'adresse MAC manuellement ou la sélectionner dans la liste des clients DHCP.

Menu Pare-Feu - Blocage URL

Le routeur ADSL SAGEM F@st 1500WG permet de bloquer l'accés à certains sites Web depuis un PC donné en saisissant ici des noms de sites ou seulement des mots clés. Cette fonction peut être utilisée pour protéger les enfants de l'accès à des sites violents ou pornographiques.

Cette page permet de définir jusqu'à 30 sites.

Pour spécifier un PC particulier, revenez à la page **Contrôle de l'accès** puis cochez la case en regard de **WWW avec blocage d'URL** et saisissez l'adresse IP (ou une plage d'adresses) du PC concerné.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
» Contrôle de l'accès
» Filtre Mac
» Blocage d'URL
» Réglage de l'horaire
» Détection des intrusions
» DMZ

Blocage d'URL

Sites Web et mots clés non autorisés.

Numéro de la règle	URL / Mot clé	Numéro de la règle	URL / Mot clé
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 14		Site 29	
Site 15		Site 30	

Effacer tout — Aide — Appliquer — Annuler

Menu Pare-Feu - Réglage de l'horaire

Vous pouvez bloquer l'accès Internet pour certains clients de votre réseau pour une ou plusieurs applications suivant des règles d'horaire.

Cliquez sur **Ajouter une règle** pour créer une nouvelle règle.

Puis appliquez cette règle dans la page **Contrôle de l'accès**.

Le routeur ADSL SAGEM F@st 1500WG permet de créer 10 règles.

Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
» Contrôle de l'accès
» Filtre Mac
» Blocage d'URL
» Réglage de l'horaire
» Détection des intrusions
» DMZ

Réglage de l'horaire

- Tableau de Régles Programmés (10 régles au maximum)

Nom de la règle	Commentaire sur la règle	Configurer
8h--18h	Blocage 8h à 18h	Modifier Supprimer
Total mercredi	Total mercredi	Modifier Supprimer
Nuit1	Nuit1 22-24	Modifier Supprimer
Nuit2	Nuit2 0-7	Modifier Supprimer
Week end	Week end	Modifier Supprimer

Ajouter une règle d'horaire

Aide Appliquer Annuler

Menu Pare-Feu - Réglage de l'horaire - Ajouter une règle

Définissez la configuration appropriée pour cette règle.

L'exemple permet un blocage les Samedi et Dimanche, toute la journée.

Pour interdire l'accès la nuit (de 18h à 7h par ex) vous devez créer 2 règles : 18-24 et 0-7.

Puis, cliquer sur **Valider**.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
» Contrôle de l'accès
» Filtre Mac
» Blocage d'URL
» Réglage de l'horaire
» Détection des intrusions
» DMZ
Routage
QoS
Avancé

Modifier la règle d'horaire

Nom: Week end

Commentaire: Week end

Activate Time Period:

Semaine Jour	Heure de début (hh:mm)	Heure de fin (hh:mm)
Tous les jours	00 : 00	00 : 00
Dimanche	00 : 00	24 : 00
Lundi	00 : 00	00 : 00
Mardi	00 : 00	00 : 00
Mercredi	00 : 00	00 : 00
Jeudi	00 : 00	00 : 00
Vendredi	00 : 00	00 : 00
Samedi	00 : 00	24 : 00

Valider Annuler

Menu Pare-Feu - Détection des intrusions (1)

1 - Détection des intrusions .

La fonction **Détection des intrusions** comprend deux parties importantes :

- Le SPI (Stateful Packet Inspection) - Limite l'accès du trafic entrant sur le port WAN.
- La prévention des attaques de pirates (Anti-DoS) - Examine le contenu des paquets de la couche application, maintient les informations de session TCP et UDP, y compris le temps maximum d'inactivité et le nombre de sessions actives et permet de détecter et d'empêcher certains types d'attaques de réseau (Anti-DoS).

Problème de RIP - Si un paquet RIP n'est pas acquitté par le routeur, il restera dans la file d'attente et ne sera pas libéré. Celà peut être la source de problèmes graves.

Ignorer le ping vers le WAN - Interdit tout ping entrant sur le port WAN du routeur.

La prévention des attaques par déni de service (DoS) protège le réseau local contre les attaques suivantes :

IP Spoofing
Land Attack
Ping of Death
IP with zero length
Smurf Attack
UDP port loop-back
Snorf Attack
TCP null scan
TCP SYN flooding.

Pare-Feu
» Contrôle de l'accès
» Filtre Mac
» Blocage d'URL
» Réglage de l'horaire
» Détection des intrusions
» DMZ
Routage

Détection des intrusions

• Fonction de détection des intrusions

Protection avec pare-feu SPI et Anti-DoS	☑
Problème de RIP	☐
Ignorer le ping vers le WAN	☐

Menu Pare-Feu - Détection des intrusions (2)

2 - Stateful Packet Inspection.

Cette fonction examine le contenu des paquets en relation avec les protocoles des différentes couches OSI pour déterminer l'état de la communication. Les données provenant du WAN ne sont autorisées à passer le pare-feu que si elles font partie d'une session initialisée par un utilisateur depuis le réseau local.

Quand la fonction SPI du pare-feu est activée, tous les paquets entrants peuvent être bloqués, sauf si certains types de trafic sont cochés par l'utilisateur. Par exemple, si l'utilisateur coche seulement **Service FTP**, dans cette page, tout le trafic entrant sera bloqué sauf pour les connexions FTP initiées par le LAN.

SPI vous permet de sélectionner plusieurs types d'applications utilisant des numéros de ports dynamiques.

Pour activer cette fonction, cocher la case **Protection avec pare-feu et Anti-DoS** et sélectionnez le type d'inspection que vous désirez dans l'écran ci-dessous.

Menu Pare-Feu - Détection des intrusions (3)

3 - Envoi d'un email sur intrusion.

Remplissez tous les champs pour être prévenu par email en cas d'intrusion.

- **Si des pirates informatiques tentent d'accéder à votre réseau, nous pouvons vous avertir par e-mail.**

Votre adresse e-mail :

Adresse du serveur SMTP :

Adresse du serveur POP3 :

Nom d'utilisateur :

Mot de passe :

Menu Pare-Feu - Détection des intrusions (4)

4 - Stratégie de connexion.

Saisissez les valeurs appropriées :

• Stratégie de connexion			Limites :
Attente de fragmentation à demi ouverte:	10	secondes	1..120
Attente TCP SYN:	30	sec.	1..120
Attente TCP FIN:	5	sec.	1..60
Temps maximum d'inactivité de la connexion TCP:	3600	sec.	1800..7200
Temps maximum d'inactivité de la session UDP:	30	sec.	1..120
Temps maximum d'inactivité du canal de données H.323:	180	sec.	

Menu Pare-Feu - Détection des intrusions (5)

5 - Critères de détection d'un DoS (Denial of Service) et du balayage de ports.

Le pare-feu n'altère pas de façon signiticative les performances du routeur, aussi, nous vous conseillons d'activer cette fonction pour protéger votre réseau.

- **Critère de détection d'un DoS:**

Paramètre	Valeur	Unité	Limites :
Total ELEVE de sessions TCP/UDP incomplètes:	300	session	1..300
Total BAS de sessions TCP/UDP incomplètes:	250	session	1..250
Total ELEVE de sessions TCP/UDP incomplètes (par min.):	250	session	1..250
Total BAS de sessions TCP/UDP incomplètes (par min.):	200	session	1..200
Nombre maximum de sessions TCP/UDP incomplètes pour le même hôte:	10		1..50
Intervalle de temps sensible à la détection de sessions TCP/UDP incomplètes:	300	msec.	50..5000
Nombre maximum de fragmentations de paquets à demi ouvertes en provenance du même hôte:	30		1..150
Intervalle de temps sensible à la détection de fragmentation à demi ouverte:	10000	msec.	10..60000
Intervalle de blocage de piratage informatique par inondation:	300	sec.	

Menu Pare-Feu - DMZ (DeMilitarized Zone)

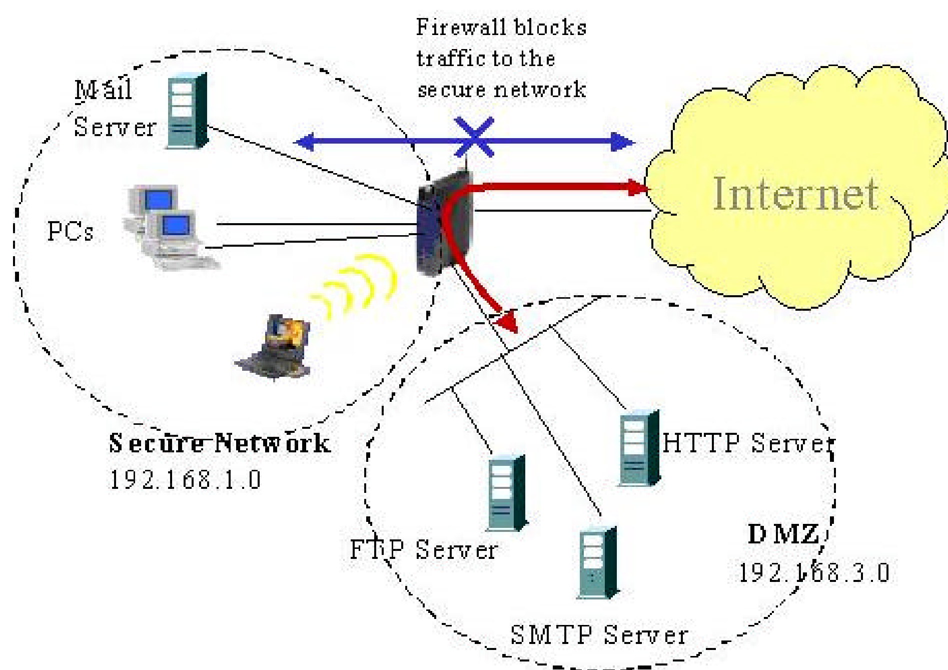
Une DMZ est un PC (ou un petit réseau) situé entre un réseau privé sécurisé et un réseau public non sécurisé (Internet). Typiquement, une DMZ supporte des applications accessibles par le WAN (serveurs Web, serveurs FTP, serveurs SMTP, jeux Internet, vidéoconférence, connexions VPN …)

Si l'un de vos PC ne peut pas exécuter une application Internet convenablement derrière votre pare-feu, vous pouvez modifier les restrictions en permettant l'accès Internet bidirectionnel.

Entrez l'adresse IP d'un hôte DMZ dans cet écran (le PC doit avoir une adresse IP fixe) et cochez la case **Appliquer**.

Grâce à votre pare-feu, vous interdisez l'accès à votre réseau sécurisé par le WAN tout en autorisant l'accès à votre DMZ.

Le routeur ADSL Sagem F@st 1500WG supporte autant de DMZ que vous avez d'adresses IP publiques.



DMZ

Activer DMZ: (•) Activer ( ) Désactiver

	Adresse IP publique	Adresse IP du PC client
1.	80.11.145.148	192.168.2.10
2.		
3.		
8.		

[Aide] [Appliquer] [Annuler]

Menu Route - Route Statique

Cet écran permet de définir des routes statiques.

Cliquer sur **Ajouter** pour ajouter une nouvelle route,

Cliquer **Modifier** pour modifier une route existante,

Cliquer **Supprimer** pour supprimer une route de la liste.

Nat
Pare-Feu
Routage
» Route statique
» RIP
» Table de routage
QoS
Avancé

Route statique

Veuillez entrer les paramètres de configuration suivants :

Index	Adresse réseau	Masque de sous-réseau	Passerelle	Configurer
1	192.168.10.0	255.255.255.0	192.168.2.1	Modifier Supprimer
2	10.10.0.0	255.255.0.0	192.168.2.1	Modifier Supprimer

Ajouter

Aide Appliquer Annuler

Index : Numéro de l'entrée.

Adresse réseau : Adresse réseau de la route. Une adresse 0.0.0.0 et un masque de 0.0.0.0 correspondent à la route par défaut.

Passerelle : Adresse IP WAN de la passerelle du réseau distant.

Menu Route - RIP (Routing Information Protocol)

L'appareil prend en charge le protocole RIP v1 et v2 pour échanger dynamiquement des informations de routage avec les routeurs adjacents. RIPv2 se distingue de RIPv1 par l'ajout des 3 champs suivants :
Route Tag : permet de faire la distinction entre les routes internes apprises nativement par RIP des routes externes apprises par un autre protocole de routage.
Subnet mask : masque de sous-réseau, s'applique à l'adresse annoncée.
Next-Hop : indique l'adresse IP du prochain équipement à joindre pour atteindre l'adresse.

RIP mode : Pour activer ou désactiver RIP.

Synthèse auto : Avec l'option **Regroupement automatique de routes**, plusieurs routes vers des sous-réseaux appartenant à un même super-réseau peuvent être remplacées par une seule route vers ce super-réseau, ce qui permet d'économiser de la place dans la table de routage.

Interface: Interface WAN à configurer.

Mode d'opération :
- Désactiver : RIP est désactivé sur cette interface.
- Activer : RIP est activé sur cette interface.
- Silencieux : Ecoute les broadcasts et met sa table de routage à jour sans rediffuser les informations.

Version: Version à utiliser sur l'interface. Les versions 1 et 2 sont prises en charge.

Poison Reverse : Le **Retour empoisonné** permet de réannoncer la route apprise par un routeur à celui-ci en lui affectant une métrique infinie (16) afin de lui signifier que le chemin n'est pas à utiliser. Cette méthode permet de casser les boucles de routage.

Authentication Required : Avec RIP v2, il est possible d'utiliser un mécanisme d'authentification pour assurer la sécurité de l'échange des tables de routage.
Cette méthode est peu sécurisée car il est possible de voir la clé d'authentication dans les paquets RIP.

Authentication Code : Mot de passe.

RIP

Veuillez entrer les paramètres de configuration suivants :

- RIP Paramètres Généreaux:
  - RIP mode: ◉ Désactiver ○ Activé
  - Synthèse auto: ◉ Désactiver ○ Activé
- Table des paramètres RIP d'interface courants :

Interface	Mode d'Opération	Version	Poison Reverse	Authentication Required	Authentication Code
VLAN1 (Default)	Désactiver	1	Désactiver	Sans	
ATM1	Désactiver	1	Désactiver	Sans	
ATM2	Désactiver	1	Désactiver	Sans	
ATM3	Désactiver	1	Désactiver	Sans	
ATM4	Désactiver	1	Désactiver	Sans	
ATM5	Désactiver	1	Désactiver	Sans	
ATM6	Désactiver	1	Désactiver	Sans	
ATM7	Désactiver	1	Désactiver	Sans	
ATM8	Désactiver	1	Désactiver	Sans	
PPPoE1	Désactiver	1	Désactiver	Sans	
PPPoE2	Désactiver	1	Désactiver	Sans	
PPPoE3	Désactiver	1	Désactiver	Sans	
PPPoE4	Désactiver	1	Désactiver	Sans	
PPPoE5	Désactiver	1	Désactiver	Sans	
PPPoE6	Désactiver	1	Désactiver	Sans	
PPPoE7	Désactiver	1	Désactiver	Sans	
PPPoE8	Désactiver	1	Désactiver	Sans	



Menu Route - Table de routage

Table de routage dynamique. Plusieurs types de routes sont prises en charge (indicateur).

Indicateur C = Directement connecté sur le même sous-réseau,
S = Route Statique,
R = Route apprise par RIP (Routing Information Protocol),
I = Redirection ICMP (Internet Control Message Protocol).

Adresse réseau Adresse IP destination.

Masque Associé à l'adresse IP destination, permet d'identifier l'adresse du réseau et l'adresse de l'hôte.

Passerelle Adresse IP du routeur vers lequel la trame sera envoyée.

Interface Interface locale utilisée pour atteindre le routeur.

Métrique Compteur lié au paquet RIP. Il s'incrémente de 1 à chaque fois que le paquet passe par un routeur. Les valeurs valides sont comprises entre 1 et 15. La valeur 16 indique une mauvaise route (poison reverse).

Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
» Route statique
» RIP
» Table de routage
QoS
Avancé

Table de routage

Le contenu de la La table de routage dynamique :

Indicateurs	Adresse réseau	Masque	Passerelle	Interface	Métrique
C	0.0.0.0	0.0.0.0	directement	ATM1	---
S	10.10.0.0	255.255.0.0	192.168.2.1	VLAN1	---
C	80.11.145.1	255.255.255.255	directement	ATM1	---
C	80.0.0.0	255.0.0.0	directement	ATM1	---
S	192.168.10.0	255.255.255.0	192.168.2.1	VLAN1	---
C	192.168.2.0	255.255.255.0	directement	VLAN1	---
C	127.0.0.1	255.255.255.255	directement	Bouclage	---

Menu QoS

Un déséquilibre de bande passante entre le LAN et le WAN peut significativement dégrader la performance des applications critiques telles que la voix sur IP, les jeux interactifs sur Internet et le service VPN...
Cette fonctionnalité de la QoS permet aux utilisateurs de classifier le trafic des applications et de leur fournir des services différenciés basés sur le protocole Diffserv.

Saisir le **Minimum garanti** pour chaque service et cocher la case **Dépassement** si besoin.

Note : Si le **Minimum garanti** est 0% avec la case **Dépassement** non cochée, celà revient à bloquer le trafic pour le service concerné.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
» Trafic associé
» Statistiques de trafic
Avancé

Configurer la QoS

Activer ou désactiver la fonctionnalité de la QoS : ○ Activer ◉ Désactiver

Groupes de services différenciés Diffserv :

Nom	Description	Priorité	Allocation de bande passante	
			Minimum garanti	Autoriser à dépasser les minimums de bande passante garantie allouée
BE	Le service au mieux, sans garantie (BE) sur les paquets à acheminer	Le plus faible	10 %	☐
AF1x	Le service à acheminement garanti (AF) assure l'acheminement des paquets à travers 4 classes d'acheminement distinctes AF1x, AF2x, AF3x, AF4x. Dans chaque classe AF, un paquet IP peut être assigné à un des 3 différents niveaux de priorité.	Faible ↑ ↓ Fort	0 %	☐
AF2x			20 %	☐
AF3x			0 %	☐
AF4x			30 %	☐
EF	Le service à traitement accéléré (EF) est destiné à assurer une garantie de bande passante et à minimiser la latence (délai de traversée du réseau), la variation de cette latence (gigue), le taux de perte des paquets acheminés.	Le plus faible fort	40 %	☑

Menu QoS - Trafic associé (1)

Jusqu'à 16 règles de classification de trafic peuvent être définies.

Le service au mieux, sans garantie (BE) sur les paquets à acheminer

Le service à acheminement garanti (AF) assure l'acheminement des paquets à travers 4 classes distinctes. Dans chaque classe AF, un paquet IP peut être assigné à un des 4 différents niveaux de priorité d'élimination. En cas de congestion, le niveau de priorité contenu dans l'entête IP du paquet détermine l'importance du paquet dans la classe AF. Le routeur tente alors de préserver les paquets IP avec un niveau de priorité de valeur faible, en éliminant prioritairement les paquets avec un niveau de priorité de valeur élevée.

Le service à traitement accéléré (EF) est destiné à assurer une garantie de bande passante et à minimiser la latence (délai de traversée du réseau), la variation de cette latence (gigue), le taux de perte des paquets acheminés.

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
» Trafic associé
» Statistiques de trafic

Trafic associé

Nom de la règle	Description du trafic	Associer à un groupe de services Diffserv	VC sortant	Configure
Telnet	TELNET	BE	by routing	Modifier Supprimer Non opérationnel
Surf	WWW	AF4x	by routing	Modifier Supprimer Monté Non opérationnel
FTP	FTP	EF	by routing	Modifier Supprimer Monté

Ajouter une classe de trafic

Aide

Menu QoS - Trafic associé (2) - Ajouter une classe de trafic

Cette page permet à l'utilisateur de spécifier une règle de classification.
En premier, définir la classe par le type de trafic.
Si nécessaire, saisir l'adresse en local et celle du distant en cliquant sur le bouton **Configuration avancée**.
Associer ensuite cette classe à un groupe de service Diffserv.
Choisir enfin le VC sortant par lequel le trafic de cette classe sera acheminé.
La règle de classification est à présent appliquée sur tous les nouveaux flux entrants.

Editer une classe de trafic

Nom de la règle		
Type de trafic	N'importe lequel	Configuration avancée
Associer à un groupe de service	BE	Re-changer DSCP
Affecter à un VC	Par routage	

Configuration avancée

L'adresse en local	Astérisque
L'adresse du distant	Bornes IP
	0 . 0 . 0 . 0 ~ 0

Type de trafic
N'importe lequel
FTP
VoIP
E-MAIL
SNMP
TELNET
WWW
VPN
TCP défini par l'utilisateur
UDP défini par l'utilisateur
IP défini par l'utilisateur

L'adresse en local
La MAC adresse
Bornes IP
Ce routeur
Astérisque

L'adresse du distant
Bornes IP
Astérisque

Menu QoS - Statistiques de trafic

Cette page affiche les statistiques du trafic du WAN pour tous les groupes de services Diffserv des 12 dernières heures (une mise à jour automatique est effectuée toutes les 5 minutes).

Information
Configuration
Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
» Trafic associé
» Statistiques de trafic
Avancé

Forwarding Behavior	Average sent byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	1389	191	32	16
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	65	33	5	3
EF	22	3	1	0

Forwarding Behavior	Average dropped byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	59	10	5
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	0	0	0	0

SAGEM F@st™ 1500WG

- Généralités F@st 1500WG
- Description physique
- Installation du modem routeur
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP



Menu Avancé - ADSL

Cette page vous permet de spécifier le standard ADSL à utiliser.

Vous pouver définir un standard spécifique explicitement ou choisir **Automatique** pour négocier automatiquement avec le DSLAM distant.

ADSL

Mode d'Opération: Automatique

Mode d'Opération
Automatique
T1.413 Issue 2
G.992.1 (G.DMT)
G.992.2 (G.Lite)

Index de suivi :

- Etat:

	Configuré	Courant
Etat de la ligne	---	SHOWTIME
Type de liaison	---	Chemin entrelacé

- Débit de données :

Type de communication	Débit de données réel
Emission	160 (Kbps.)
Réception	608 (Kbps.)

- Données de fonctionnement / Indication d'anomalie :

Données de fonctionnement	Emission	Réception
Marge de bruit	31 dB	19 dB
Atténuation	60 dB	48 dB

Nom de l'indicateur	Indicateur de paradiaphonie	Indicateur de télédiaphonie
Correction FEC rapide	0	0
Correction FEC entrelacée	0	86
Erreur de CRC rapide	0	0
Erreur de CRC entrelacée	5	0
Défaut de type perte du signal	0	---
Erreur HEC rapide	0	0
Erreur HEC entrelacée	204	0

- Statistiques:

Cellules reçues	588028
Cellules transmises	66160

Menu Avancé - Gestion à distance

La gestion à distance depuis un port WAN peut être interdite (défaut), autorisée ou limitée à un hôte distant donné.

Une adresse IP 0.0.0.0 correspond à n'importe quel hôte.

Cochez la case **Activé**, saisir éventuellement l'adresse de l'hôte et cliquez sur **Appliquer**.

Vous pouvez changer le numéro de port par défaut (8080).

Pour utiliser TELNET, vous devez également autoriser la configuration à distance.

Dans ce cas, le port par défaut est 8081. Il est modifiable par TELNET.

Nat
Pare-Feu
Routage
QoS
Avancé
» ADSL
» Gestion à distance
» SNMP
» UPnP
» DDNS

Gestion à distance

Définition de la gestion à distance du routeur. Si vous souhaitez gérer le routeur depuis un emplacement distant (hors du réseau local), vous devez aussi spécifier l'adresse IP du PC distant.

Activé	☑
Adresse hôte	0.0.0.0
Masque de sous-réseau	255.255.255.0
Numéro de port	8080

Aide | Appliquer | Annuler

Menu Avancé - SNMP - Communauté

Simple **N**etwork **M**anagement **P**rotocol est un protocole de la couche application qui facilite l'échange des informations de gestion entre les appareils du réseau. Il s'appuie sur le protocole de niveau transport **UDP** (non connecté donc non fiable).

SNMP permet aux administrateurs de :

- Contrôler un équipement à distance,
- Interroger un équipement sur son état,
- Modifier l'état d'un équipement,
- Faire des tests et des statistiques.

Chaque appareil appartient à une **Communauté** identifiée par son nom (par défaut : **public**).
Ce nom fournit un niveau de sécurité très basique puisque vous avez besoin de le connaître pour communiquer avec l'appareil mais qu'il circule en clair sur le réseau.

Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
Avancé
» ADSL
» Gestion à distance
» SNMP
» UPnP
» DDNS

SNMP

Dans le contexte SNMP, une relation entre un agent et un ensemble de gestionnaires SNMP définit les caractéristiques de sécurité. Le concept de communauté est un concept local, défini au niveau de l'agent. L'agent établit une communauté pour chaque combinaison souhaitée d'authentification, contrôle d'accès et caractéristiques proxy. Un nom de communauté unique (pour cet agent) est attribué à chaque communauté et les stations de gestion de cette communauté sont informées de ce nom, qu'elles doivent utiliser dans toutes les opérations de saisie. L'agent peut établir plusieurs communautés, avec un chevauchement possible des membres des stations de gestion.

Num.	Communauté	Version	Valider
1	public	Lire	☑
2	private	Ecrire	☐
3		Lire	☐
4		Lire	☐
5		Lire	☐

Menu Avancé - SNMP - Trap SNMP

Un **Trap** est un message non sollicité envoyé par un agent **SNMP** à un système de gestion de réseau (**NMS**) pour signaler l'apparition d'un événement significatif.

Spécifiez l'adresse IP de votre station **NMS** et cliquez sur **Appliquer**.

Système
Réseau Distant
Réseau Local
Réseau Sans Fil
Nat
Pare-Feu
Routage
QoS
Avancé
» ADSL
» Gestion à distance
» SNMP
» UPnP
» DDNS

Trap SNMP

Dans le contexte SNMP, un agent peut envoyer un message spontané à une station de gestion. Le but est d'aviser la station de gestion d'un événement inhabituel.

Num.	Adresse IP	Communauté	Version
1			Désactivé
2			Désactivé
3			Désactivé
4			Désactivé
5			Désactivé

Aide Appliquer Annuler

Menu Avancé - UPnP (Universal Plug and Play)

La technologie **UPnP** est un protocole qui permet de relier sans aucun effort plusieurs ordinateurs et autres équipements informatiques entre eux.

Elle utilise des standards bien connus comme TCP/IP et HTML pour permettre de découvrir des équipements et les services disponibles sur votre réseau.

UPnP va aussi permettre d'exercer un contrôle sur certains équipements de votre réseau interne.

Cliquer sur **Activer** pour activer la fonction UPNP sur le routeur.

Cliquer sur **Appliquer**.

Routage
QoS
Avancé
» ADSL
» Gestion à distance
» SNMP
» UPnP
» DDNS

UPnP

L'architecture de UPnP(Universal Plug and Play) vous donne une facilité de connexion point à point de votre ordinateur avec toute sorte de facteurs, appliances intelligentes, et des périphériques sans fil. UPnP peut aussi vous donner la possibilité de piloter votre réseau et le transfert de données depuis votre domicile, bureau ou ailleurs.

Activer ou désactiver la fonctionnalité de UPnP: Activer Désactiver

Aide Appliquer Annuler

Menu Avancé - DDNS (DNS Dynamique)

Le **DDNS** permet aux utilisateurs d'associer un nom de domaine statique à une adresse IP dynamique. Vous devrez obtenir un compte, un mot de passe et votre nom de domaine statique fournis par un fournisseur de service DDNS. Ce routeur supporte les services DDNS fournis par www.dyndns.org and www.tzo.com.

Configurez cet écran en renseignant tous les champs puis cliquez sur **Appliquer**.

Vérifiez le message suivant dans le **Journal des connexions** de la page **Information**.

07/13/2005 09:15:40 DDNS> Operation complete, DDNS IP=80.11.145.186

Ce message indique que l'opération s'est déroulée correctement. Par contre, le message suivant indique qu'il y a une erreur dans un de vos paramètres.

07/13/2005 09:05:22 DDNS> Invalid Account(username or password)

Avec le DDNS activé, vous pouvez maintenant construire votre propre site web, site FTP et d'autres, tout en ayant une adresse IP dynamique. Ce service permet aux utilisateurs de retrouver votre site.

Exemple : c:\>ping sagem2.dyndns.org
Envoi d'une requête 'ping' sur sagem2.dyndns.org [80.11.145.53] avec 32 octets de données :
Réponse de 80.11.145.53 : octets=32 temps=110 ms TTL=62

Routage
QoS
Avancé
» ADSL
» Gestion à distance
» SNMP
» UPnP
» DDNS

Configurer le DDNS (Dynamic DNS)

DNS Dynamique	Activer / Désactiver
Fournisseur d'accès	DynDNS.org
Nom du domaine	sagem2.dyndns.org
Compte / E-mail	sagem
Mot de passe / Clé	●●●●●

SAGEM F@st™ 1500WG

- Généralités F@st 1500WG
- Description physique
- Installation du modem routeur
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP

Alarmes de fonctionnement

- Ces alarmes correspondent à des événements qui apparaissent dans le fonctionnement du routeur SAGEM F@st™ 1500WG (1540) .
  Ils peuvent être diagnostiqués grâce aux LED.
- Le tableau suivant précise la signification de ces voyants.

Marquage	PWR	ADSL	WLAN	ALM	ETHERNET
Affectation	Alimentation	Liaison ADSL	Liaison WLAN	Liaison PPP	Liaison ETHERNET
Allumé fixe	SAGEM F@st™ 1500 sous tension	ADSL connectée	Réseau sans fil opérationnel	Liaison PPP non établie	Liaison ETHERNET établie
Eteint	Pas d'alimentation	ADSL non actif et pas de DSLAM détecté	Réseau sans fil non opérationnel	Liaison PPP étabie	Liaison ETHERNET non établie
Clignotant	X	Synchronisation ADSL en cours	X	X	Traffic sur le lien ETHERNET



Dépannage

- <u>LED **WLAN** éteinte</u>
  - L'interface WLAN du routeur SAGEM F@st™ 1500WG (ou 1540WG) n'est pas opérationnelle.
    - Vérifiez la configuration du réseau sans fil.
- <u>LED **ETH** éteinte</u>
  - L'interface Ethernet du routeur n'est pas connectée à une interface Ethernet distante active.
    - Vérifiez que le routeur est connecté à un équipement actif (carte Ethernet ou hub) par un câble droit ou croisé (auto détection).
    - Vérifiez que le cordon Ethernet est correctement enfiché aux 2 extrémités
    - Vérifiez que les broches des connecteurs RJ45 ne sont ni sales ni endommagées.
- <u>LED **ADSL** clignotante</u>
  - Le routeur tente de se synchroniser avec le DSLAM distant.
    Cet indicateur reste dans cet état tant que le routeur n'est pas connecté à une ligne ADSL active.
  - La connexion ADSL prend moins d'une minute à partir de la mise sous tension.
    - Vérifiez que le routeur est connecté correctement à une ligne ADSL.
    - Vérifiez que les broches des connecteurs RJ11 ne sont ni sales ni endommagées.
    - Vérifiez auprès de votre FAI que le mode ADSL est bien activé sur la ligne que vous désirez utiliser.
- <u>LED **ALM** allumée</u>
  - Le PPP n'est pas établi.
    - Vérifiez les paramètres de LOGIN.
    - Vérifiez les paramètres ATM (protocol, VPI/VCI, encapsulation).

SAGEM F@st^{TM} 1500WG

- Généralités F@st 1500WG
- Description physique
- Installation du modem routeur
- Configuration du modem routeur
- Installation des modules Wi-Fi
- Configuration du NAT, Firewall, Route & QoS
- Configuration avancée
- Etude des problèmes éventuels
- Configuration IP

IP Configuration

Votre PC doit être configuré en mode **DHCP** (ou en adresse IP fixe si vous utilisez des serveurs locaux)

Procédez comme suit :

- Ouvrez l'écran **Propriétés du Protocole Internet (TCP/IP)**,
- Configurez comme ci-dessous,
- En adresse IP fixe, renseignez les champs **Passerelle par défaut** et **Serveur DNS**.

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

(•) Obtain an IP address automatically
( ) Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

(•) Obtain DNS server address automatically
( ) Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

Propriétés de Protocole Internet (TCP/IP)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

( ) Obtenir une adresse IP automatiquement
(•) Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 2 . 10
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 2 . 1

( ) Obtenir les adresses des serveurs DNS automatiquement
(•) Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 80 . 10 . 245 . 1
Serveur DNS auxiliaire : 80 . 10 . 245 . 2

Avancé...

OK | Annuler

Configuration IP

Pour vérifier votre configuration TCP / IP vous devez procéder comme suit :

] Ouvrir une fenêtre de commande DOS

] menu démarrer / exécuter

] taper **cmd** dans la fenêtre ouverte (pour Win XP ou Win 2000, **winipcfg** pour Win 98)

Une fenêtre de commande DOS apparaît :

Dans cette fenêtre, vous avez le choix entre plusieurs commandes:

] **ipconfig /all** pour obtenir la configuration TCP/IP complète de votre PC

] **ipconfig /release** pour libérer l 'adresse IP donnée par le serveur DHCP

] **ipconfig /renew** pour renouveler l'adresse IP donnée par le serveur DHCP

] **ping** pour vérifier le lien avec l'adresse IP d'un ordinateur

Voir les écrans suivants :

IP Configuration

ipconfig /all : Pour vérifier la configuration IP de toutes vos interfaces

```
c:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : P1198210
        Primary DNS Suffix. . . . . . . . :
        Node Type . . . . . . . . . . . . : Broadcast
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connection
        Physical Address. . . . . . . . . : 00-A0-D1-D6-74-99
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.0.0.211
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . : 10.0.0.136
        DHCP Server . . . . . . . . . . . : 10.0.0.136
        DNS Servers . . . . . . . . . . . : 80.10.246.1
                                          : 80.10.246.132
        Lease Obtained. . . . . . . . . . : Monday, January 3, 2005 08:31:45 AM
        Lease Expires . . . . . . . . . . : Monday, January 3, 2005 08:31:45 PM
```

ipconfig /release : Pour libérer l'adresse attribuée par le serveur DHCP

```
c:\>ipconfig /release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"
```

IP Configuration

ipconfig /renew : Pour redemander une nouvelle adresse IP au serveur DHCP

```
c:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix. . :
        IP Address. . . . . . . . . . . . : 10.0.0.211
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . : 10.0.0.136
```

Ping : pour vérifier l 'accessibilité à l 'adresse IP d 'un autre équipement.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data :

Reply from 192.168.1.1 : bytes=32 time<10 ms TTL=254
Reply from 192.168.1.1 : bytes=32 time<10 ms TTL=254
Reply from 192.168.1.1 : bytes=32 time<10 ms TTL=254
Reply from 192.168.1.1 : bytes=32 time<10 ms TTL=254

Ping statistics for 192.168.1.1:
    Packets : sent = 4, Received = 4, Lost = 0 (0%Loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



GLOSSAIRE



Glossaire

- **NETWORK :**
  Connection of several machines. It can be a private network (enterprise) or a public network (Internet). Rules of communication between machines are defined in protocols (IP for example).
- **INTERNET :**
  World-wide network shared between millions of users.
- **INTRANET :**
  A solution to broadcast private content into a company with the same technology as Internet (PC, Server, Network) on a private network (for example) providing contents to employees.
- **EXTRANET :**
  A solution to broadcast private content to a specific list of user through Internet access.
  It uses the same technology as Internet (PC, Server, Network).
- **IP - Internet Protocol :**
  The protocol that makes Internet possible ! It enables all PCs and terminal to access to all servers by sharing the transport network. Technically speaking it's a level 3 protocol, like a mail with a stamp explaining the source and the destination of information.
- **ADSL :**
  Technology enabling the operator to convey Internet on the phone line up to the end user.
- **ETHERNET :**
  Type of interface between equipment. Technically speaking, it's a frame that contain data (IP frame) so information over a network.

Glossaire

- **MODEM:** A equipment located in the end user facility and connected to the phone line or to a metropolitan access.
  It does exist several types of modems: V92 (regular one), ADSL modem, Cable modem, ….
- **ROUTER:** A machine or a function that enable the user to connect several PCs or terminals.
- **DSLAM:** **Digital Subscriber Line Access Multiplexer**
  Central office equipment enabling to connect a great number of end-user.
  They are located near the public exchange.
- **BAS:** **Broadband Access Server**
  Equipment managed by operator or ISP to control access of users on Internet.
  It enables operator and ISP to authenticate and to bill the end-user. BAS are connected to the subscribers information system (end of the PPP session for login/password).
- **WiFi:** **Wireless Fidelity**
  Wireless Fidelity, it's alliance of competitors using wireless 802.11x technology
- **802.11x:** Technology that enables to transport Ethernet data on the air.
- **Bluetooth:** A wireless personal area network (PAN) using omni-directional radio waves that can transmit through walls and other non-metal barriers.

Glossaire

- **Hotspot :** Public place like airport, hotel or railway station equipped with wireless access point and making possible to access Internet with your PC laptop.
- **USB :** **Universal Serial Bus**
  Interface designed to exchange information between computer and peripherals (like printer, modem, camera, and so on).
- **CPE :** **Customer Premises Equipment** . This is your broadband modem..
- **SOHO :** Small Office Home Office (less than 10 terminals).
- **PSTN :** Public switched Telephone Network.
- **ISDN :** Integrated Services Data Network.
- **PPP :** **Point to Point Protocol**
  Protocol for Authenticate a remote machine throughout a access network.
  Associated protocols are PAP/CHAP for Authentication, IPCP for affecting address.
- **DHCP** : **Dynamic Host Control Protocol**
  Protocol that enable terminals to get their IP address.
  An handshake with a server define the IP address and other parameters.
- **DNS :** **Domain Name Server**
  A server that enables to match IP address and a name according the syntax:
  firstname.lastname@domainname.domain.
- **TCP :** **Transmission Control Protocol**
  Protocol to transmit data in safe manner between two points of an IP network.

Glossaire

- **UDP:** **User Datagram Protocol**
  Very simple protocol without protection against loss.
- **FTP:** **File transfer protocol**
  Protocol enabling to exchange file between two points of an IP network.
- **NAT/PAT:** Network Address Translation /Port Address Translation enabling a device.
- **TFTP:** **Trivial File Transfer protocol**
  The simplest way to download a new firmware in a modem or a router.
- **COMBO:** Modem with 2 interfaces (USB and Ethernet for example).
  It's not a router.
- **SNMP:** **Simple network management protocol**
  It defines the transmission of information between a device and a management application.
  Device sends "trap" to inform the management application
  (the operator of the network) that something happens
  (change of configuration, alarms, remote default, …)
- **CBR, VBR, UBR:**
  Constant Bit Rate, Variable Bit Rate, Unspecified BR
  Class of service of the ATM protocol.

Glossaire

- **MAC:** Media Access Control *(For Ethernet)*
- **LLC:** Logical Link Control *(For Ethernet)*
- **ARP:** Address Resolution Protocol
- **IGMP:** Internet Group Management Protocol
- **ICMP:** Internet Control Message Protocol *(between router)*
- **OSPF:** Open Shortest Path First *(Routing)*
- **RIP:** Routing Information Protocol *(Routing)*
- **SMTP:** Simple Mail Transfer Protocol *(Mail protocol)*
- **Telnet:** Teletypewriter Network Protocol *(Configuration)*
- **HTTP:** HyperText Transfer Protocol *(Basics of Internet)*
- **HTML:** HyperText Markup Language *(Format of web page)*

Glossaire

- **MGCP:** **Media Gateway Control Protocol**
  Signalling Protocol of VOIP (master/slave).
- **End Point:** User access point (phone).
- **Gateway:** This is the interface unit between the phone and IP network.
- **Call Agent:** This is the equipment connected to the gateway and which manage this one.
- **RSIP:** **Restart In Progress**
  This is the gateway which inform the Call Agent for its voice availability.
- **AUEP:** **Audit Endpoint**
  Allow the Call Agent to detect if an end is off the hook or ready to ring.
- **RQNT:** **Request Notification**
  This is the Call Agent which asks the gateway to report any specific event (i.e.: off hook, on hook).
- **NTFY:** **Notification**
  This is the Gateway answer that means an event occurred.
- **CRCX:** **Create Connection**
  The Call Agent initiates the connection between the two ends.
- **MDCX:** **Modify Connection**
  Allows the Call Agent to modify a connection already established.
- **DLCX:** **Delete Connection**
  This is the Call Agent which allows the gateway to hang up.